456-TP-006-001

ECS Project Training Material Volume 6: Network Administration

Technical Paper

May 1997

Prepared Under Contract NAS5-60000

RESPONSIBLE ENGINEER

Mike Resnick Date
EOSDIS Core System Project

SUBMITTED BY

Tom Hickey M&O Deputy Manager Date
EOSDIS Core System Project

Hughes Information Technology Systems
Upper Marlboro, Maryland

This page intentionally left blank.

Abstract

This is Volume 6 of a series of 10 volumes containing the training material for the Pre-Release B Testbed Implementation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the process required to perform Network Administration tasks.

Keywords: training, course objective, network administration, Network Node Manager, HP OpenView

This page intentionally left blank.

Contents

Starting and Ending a NNM Session

The NNM Map and Submaps

Network Objects and Symbols

Adding a Segment Object

Adding an IP Interface Object

Viewing Current Network and System Configuration

Viewing Network Address Information

Viewing How Traffic is Routed on a Network

Viewing the Services Available on a Node

System Monitoring

Practical Exercises

Slide Presentation

Figures

Tables

This page intentionally left blank.

Introduction

Identification

Training Material Volume 6 is part of a series of Technical Papers that will be used to teach Maintenance and Operations (M&O) concepts to the M&O staff at the following Distributed Active Archive Centers (DAACs): Langley Research Center (LaRC), National Snow and Ice Data Center (NSIDC) and EROS Data Center (EDC).

Scope

Training Material Volume 6, Network Administration, is designed to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

This document reflects the August 23, 1995 Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS technical direction #11, dated December 6, 1994.

Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding network administration in the context of the ECS configuration. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics is included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

Network Administration

Lesson Overview

This lesson will provide you with the tools needed to perform the various tasks required to administer the network management portion of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations. It includes a detailed review of the procedures required to perform network management tasks as outlined below.

Lesson Objectives

Overall Objective - The overall objective of this lesson is proficiency in the basic concepts of network administration and the specific procedures of administering the Pre-Release B Testbed Implemetation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will use the Procedures Manual in accordance with prescribed methods and complete required procedures without error to accomplish all tasks required.

Specific Objective 1 - The student will be able to identify the hardware components of the local network.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will identify on sight each of the hardware components comprising the local network.

Specific Objective 2 - The student will be able to start and end a Hewlett-Packard OpenView Network Node Manager (HPOV NNM) session.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will perform without error the procedures required to start and end a HP OpenView Network Node Manager session.

Specific Objective 3 - The student will be able to add to and delete from the network map a network object, segment object, node object, and interface object.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will perform without error the procedures required to add to and delete from the network map a network object, segment object, node object, and interface object.

Specific Objective 4 - The student will be able to view current network and system configuration, network address information, traffic routing and address information.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will perform without error the procedures required to view current network and system configuration, network address information, traffic routing and address information.

Specific Objective 5 - The student will be able to configure the agent system to display network configuration and network fault status, display site computer status, monitor system performance, generate system performance reports, provide alerts to the operation staff, and log onto the computer hosts.

Condition - The student will be given a copy of 456-TP-006-001 Network Administration Student and a working system.

Standard - The student will perform without error the procedures required to configure the agent system to display network configuration and network fault status, display site computer status, monitor system performance, generate system performance reports, provide alerts to the operation staff, and log onto the computer hosts.

Importance

The Network Administration lesson will provide a review of the process that allows the Operations and Management (O&M) staff responsible for the management of network operations to configure and monitor the hardware and software components of the ECS network using the Hewlett-Packard OpenView Network Node Management software.

Network Topology

Network Hardware Components

The ECS Network topology consists a combination of data and file servers, workstations, printers, and cabling of the Ethernet and fiber optic variety. The network map below (Figure 1) shows the configuration of the Testbed network at the EROS Data Center. Similar configurations are installed at the Goddard, NSIDC and Langley Research Center DAACs..

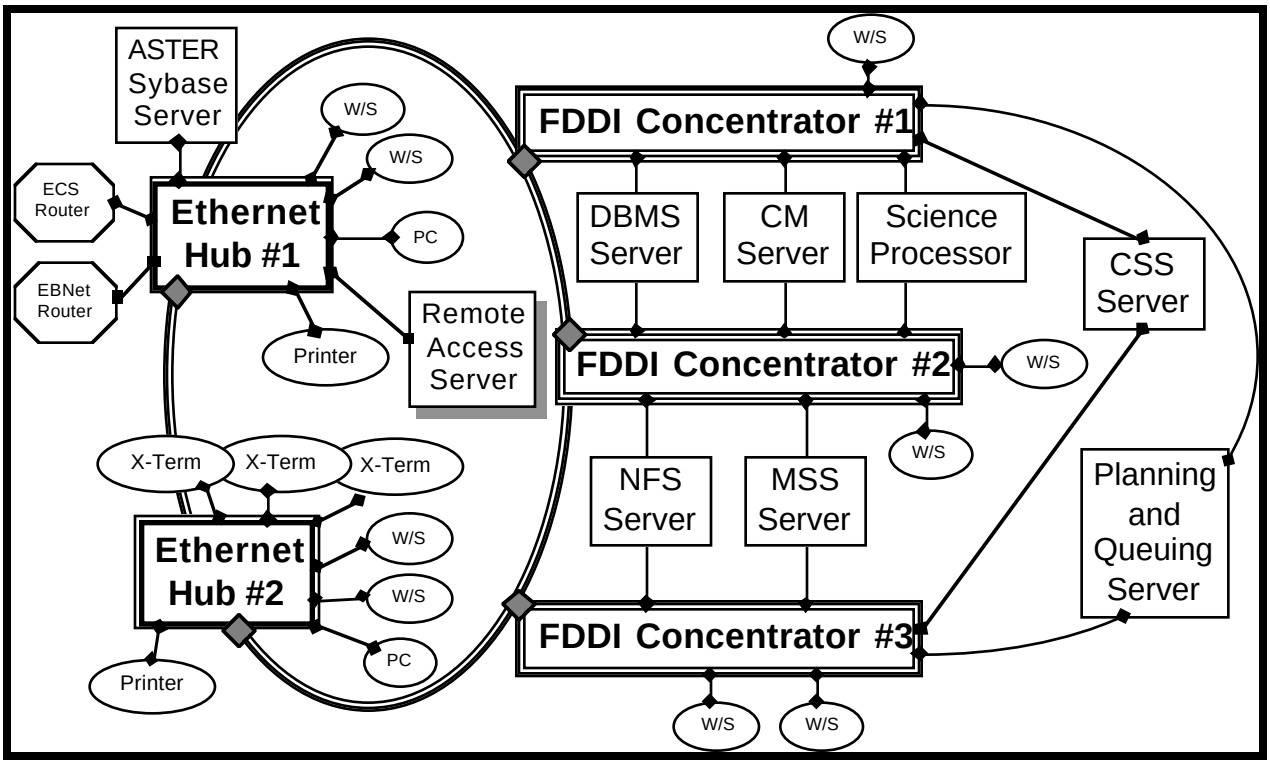

Figure 1. EDC Network Detail

Servers, Workstations, and X-Terminals

Primary among the hardware components (**Error! Reference source not found.**) of the DAAC networks are the data and file servers, workstations, and X-terminals. With such manufacturers as SGI, NCD, Sun, Solaris, and Hewlett-Packard, the variety and mix of these hardware components depends on the computing requirements of the individual DAAC.

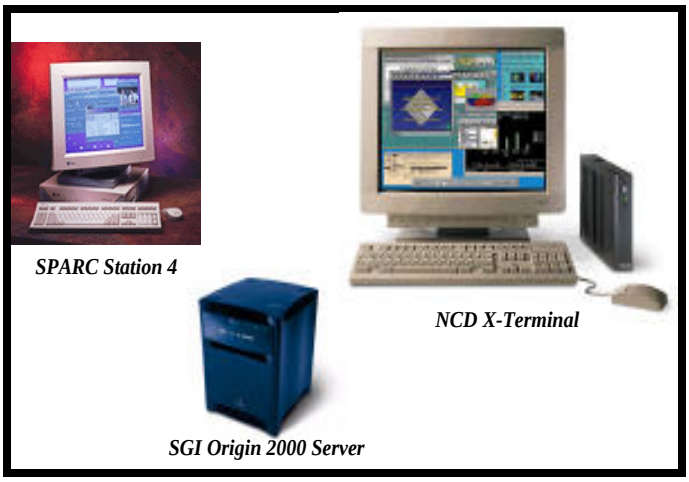

Figure 2. Sample of Network Hardware Devices

FDDI Concentrators

Figure 3. FDDI Concentrator

FDDI (Fiber Distributed Data Interface) Concentrators (Figure 3) are manufactured by SynOptics/Bay. Concentrators each have 12 ports which can route data packets between networks or switch the data packets to different legs within a single network. The FDDI connections can handle up to 100 megabits per second throughput making them among the fastest and most reliable connections available today.

Most of the FDDI networks are actually two concentric network rings running data packets in opposite directions. Thus, if one segment of a FDDI ring is disrupted, the data can still flow in the opposite direction and connect with all points on the network while maintenance is performed on the faulty segment. You will note on the DAAC network diagrams (see Appendix A) that several of the servers are connected to two FDDI concentrators on the same ring to satisfy this requirement.

10-Base-T Ethernet Hub

The Cabletron MicroMAAC-22E Ethernet-to-FDDI Hubs (Figure 4) serve to connect the FDDI ring to the ECS Router, EBNet Router, and to the Remote Access Servers and modems for dial-up access. Each hub has 12 ports plus 1 FDDI port for connection to FDDI ring.

Figure 4. 10Base-T Ethernet Hub

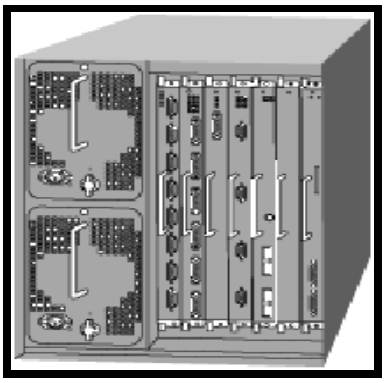

Figure 5. Cisco Series 7500 Router

Access Server, ECS Router and EBNet Router

The Cisco Series 7500 routers (**Error! Reference source not found.**) are employed on each network for connectivity to the ECS network, the EBNet network, and the public access server. Each router is responsible for moving data packets from one network to another (i.e., from on IP address to another), and for advertising IP addresses to the internet and to the local network. The routers are also responsible for maintaining a secure local environment by locking out traffic from unknown or undesirable IP addresses. Maintenance and configuration of routers is considered a non-trivial function of the network monitor. Such tasks are addressed in special technical training provided by the particular vendor and will not be discussed further in this course.

This page intentionally left blank.

IP Addresses

The IP addresses on the ECS Pre-Release B Testbed Network are Class C addresses.

The tables on the next several pages detail the IP address for each of the network hardware devices at each DAAC.

Table 1. NSIDC DAAC Pre-Release B Testbed IP Address Assignments for Network Hardware

Hardware Descriptor	Designator (diagram)	Port	Host/Device Connection	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
FDDI Concentrator	C1	mgmt	C2/C3/E1/E2	198.118.225.35	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
FDDI Concentrator	C2	mgmt	C1/C3/E1/E2	198.118.225.36	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
FDDI Concentrator	C3	mgmt	C1/C2/E1/E2	198.118.225.37	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
Ethernet Hub	E1	mgmt	C1/C2/C3/E2/ECS Router/EBnet Router	198.118.225.38	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
Ethernet Hub	E2	mgmt	C1/C2/C3/E1	198.118.225.39	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
ECS Router	ECS Router	fddi 0/0/0	NSIDC Exchange LAN	128.161.7.66	128.161.7.64	255.255.252.240	128.161.7.31	n/a
		fddi 0/1/0	Rel B User FDDI	198.118.206.65	198.118.206.64	255.255.255.192	198.118.206.127	n/a
		fddi 1/0/0	Rel B Prod. FDDI	198.118.205.1	198.118.205.0	255.255.255.0	198.118.205.255	n/a
		fddi 1/1/0	M&O Network	198.118.206.129	198.118.206.128	255.255.255.192	192.102.206.191	n/a
		e 4/1/0	Pre-Release B Testbed	198.118.225.32	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
EBnet Router	EBnet Router	?	Rel B FDDI SW/R	198.118.204.33	198.118.204.32	255.255.255.224	198.118.204.63	n/a
		?	Pre-Release B Testbed	198.118.225.33	198.118.224.32	255.255.255.224	198.118.225.63	198.118.225.34
Remote Access Server	Access Server	1	modem #1	198.118.225.41	198.118.204.32	255.255.255.224	198.118.204.63	n/a
		2	modem #2	198.118.224.42	198.118.204.32	255.255.255.224	198.118.204.63	n/a
		mgmt	E2	198.118.225.40	198.118.224.32	255.255.255.224	198.118.224.63	n/a

Table 2. NSIDC DAAC Pre-Release B Testbed IP Address Assignments for Network Hosts

Hardware Descriptor	Designator (diagram)	Port	Host Name	Concentrator or Hub ID	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
PLNHW	NSIDC-1	Planning & Queuing Server	plnn1sun	C1 & C2	198.118.225.45	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
PLNHW	NSIDC-2	Planning WS	plnn2sun	C1	198.118.225.46	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
SPRHW	NSIDC-1	Science Processor	sprn1sgi	C1 & C2	198.118.225.47	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
SPRHW	NSIDC-2	Science Processor File Server	sprn2sgi	C1 & C3	198.118.225.48	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
AITHW	NSIDC-1	SSI&T W/S	aitn1sun	C3	198.118.225.49	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
AITHW	NSIDC-2	DBMS Server	aitn2sun	C1 & C2	198.118.225.50	198.118.225.32	255.255.255.224	198.118.225.63	198.118.225.34
AITHW	NSIDC-3	HP Printer	aitn3hp	E1	198.118.225.51	198.118.225.32	225.225.225.224	198.118.225.63	198.118.225.34
MSS	NSIDC-1	MSS Server	mssn1hp	C1 & C3	198.118.225.52	198.118.225.32	225.225.225.224	198.118.225.63	198.118.225.34
MSS	NSIDC-3	MSS W/S	mssn2sun	C2	198.118.225.53	198.118.225.32	225.225.225.224	198.118.225.63	198.118.225.34
MSS	NSIDC-2	CM Server	mssn3sun	C2	198.118.225.54	198.118.225.32	225.225.225.224	198.118.225.63	198.118.225.34
CSSHW	NSIDC-1	CSS Server	cssn1hp	C1 & C2	198.118.225.55	198.118.225.32	255.255.255.224	198.118.205.63	198.118.225.34
ACMHW	NSIDC-1	NSF Server	acmn1sgi	C1 & C2	198.118.225.56	198.118.225.32	255.255.255.224	198.118.205.63	198.118.225.34
SUPP	NSIDC-1	Workstation	supn1sun	C2	198.118.225.57	198.118.225.32	255.255.255.224	198.118.205.63	198.118.225.34
SUPP	NSIDC-2	Workstation	supn2sun	C1	198.118.225.58	198.118.225.32	255.255.255.224	198.118.205.63	198.118.225.34
SE	SPARC-1	Workstation	sen1sun	E1	198.118.225.59	198.118.225.32	255.255.255.224	198.118.205.63	198.118.225.34

Table 3. EDC DAAC Pre-Release B Testbed IP Address Assignments for Network Hardware

Hardware Descriptor	Designator (diagram)	Port	Host/Device Connection	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
FDDI Concentrator	C1	mgmt	C2/C3/E1/E2	198.118.224.70	198.118.224.64	255.255.255.192	198.118.224.127	198.118.224.66
FDDI Concentrator	C2	mgmt	C1/C3/E1/E2	198.118.224.71	198.118.224.64	255.255.255.192	198.118.224.127	198.118.224.66
FDDI Concentrator	C3	mgmt	C1/C2/E1/E2	198.118.224.72	198.118.224.64	255.255.255.192	198.118.224.127	198.118.224.66
Ethernet Hub	E1	mgmt	C1/C2/C3/E2/ECS Router/EBnet Router	198.118.224.74	198.118.224.64	255.255.255.192	198.118.224.127	198.118.224.66
Ethernet Hub	E2	mgmt	C1/C2/C3/E1	198.118.224.75	198.118.224.64	255.255.255.192	198.118.224.127	198.118.224.66
ECS Router	ECS Router	fddi 0/0/0	EDC Exchange LAN	152.61.80.250	152.61.80.0	255.255.252.0	152.61.83.255	n/a
		fddi 0/1/0	NSI Router	128.161.7.18	128.161.7.16	255.255.255.240	128.161.7.31	n/a
		fddi 1/0/0	Rel B User FDDI	198.118.203.1	198.118.203.0	255.255.255.0	198.118.203.255	n/a
		fddi 1/1/0	Rel B Prod. FDDI	198.118.202.2	198.118.202.0	255.255.255.0	198.118.202.255	n/a
		fddi 4/0/0	M&O Network	192.102.216.1	192.102.216.0	255.255.255.0	192.102.216.255	n/a
		e 4/1/0	Pre-Release B Testbed	198.118.224.66	198.118.224.64	255.255.255.192	198.118.224.127	n/a
EBnet Router	EBnet Router	?	Rel B FDDI SW/R	198.118.204.33	198.118.204.32	255.255.255.224	198.118.204.63	n/a
		?	Rel B Ingest FDDI	198.118.204.65	198.118.204.64	255.255.255.224	198.118.204.95	n/a
		?	Pre-Release B Testbed	198.118.224.65	198.118.224.64	255.255.255.192	198.118.224.127	n/a
Remote Access Server	Access Server	1	modem #1	198.118.224.80	198.118.224.64	255.255.255.192	198.118.224.127	n/a
		2	modem #2	198.118.224.81	198.118.224.64	255.255.255.192	198.118.224.127	n/a
		mgmt	E1	198.118.224.76	198.118.224.64	255.255.255.192	198.118.224.127	n/a

Table 4. EDC DAAC Pre-Release B Testbed IP Address Assignments for Network Hosts

Hardware Descriptor	Designator (diagram)	Port	Host Name	Concentrator or Hub ID	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
PLNHW	EDC-1	Planning WS	plnec1sun	C2	198.118.224.82	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
PLNHW	EDC-2	Planning & Queuing Server	plnec2sun	C1 & C3	198.118.224.83	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
SPRHW	EDC-1	Science Processor	sprn1sgi	C1 & C2	198.118.224.84	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
SPRHW	EDC-2	X-Terminal	sprec2ncd	E2	198.118.224.85	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
SPRHW	EDC-3	X-Terminal	sprec3ncd	E2	198.118.224.86	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
AITHW	EDC-1	AIT WS	aitec2sun	C1	198.118.224.87	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
AITHW	EDC-2	HP Laser Printer	aitec2hp	E2	198.118.224.88	198.118.224.64	255.255.224.192	198.118.224.127	198.118.224.66
AITHW	EDC-3	AIT WS/DBMS Server	aitec3sun	C1 & C2	198.118.224.89	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
ASTER	EDC-1	LUT Sybase Server	astec1sun	E1	198.118.224.90	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
MSS	EDC-1	CM Server	mssec1sun	C1 & C2	198.118.224.91	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
MSS	EDC-2	MSS Server	mssec2hp	C2 & C3	198.118.224.92	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
MSS	EDC-3	HP Laser Printer	mssec3hp	E1	198.118.224.93	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
MSS	EDC-4	MSS WS	mssec4sun	C3	198.118.224.94	198.118.224.64	225.225.225.224	198.118.224.127	198.118.224.66
CSSHW	EDC-1	CSS Server	cssec1hp	C1 & C3	198.118.224.95	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
ACMHW	EDC-3	NSF Server	acmec1sgi	C2 & C3	198.118.224.96	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SUPP	EDC-1	Workstation	supec1sun	C3	198.118.224.97	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SUPP	EDC-2	Workstation	supec2sun	C2	198.118.224.98	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	OAWS-1	Workstation	seec1sun	E2	198.118.224.99	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	OAWS-2	Micron PC	seec2pc	E1	198.118.224.100	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	SPARC-1	Workstation	seec3sun	E1	198.118.224.101	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	SPARC-2	Workstation	seec4sun	E1	198.118.224.102	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	SPARC-3	Workstation	seec5sun	E2	198.118.224.103	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	XTERM-1	X-Terminal	seec6ncd	E2	198.118.224.104	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66
SE	OAWS-2	Micron PC	seec7pc	E2	198.118.224.105	198.118.224.64	255.255.224.192	198.118.205.63	198.118.224.66

Table 5. LaRC DAAC Pre-Release B Testbed IP Address Assignments for Network Hardware

Hardware Descriptor	Designator (diagram)	Port	Host/Device Connection	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
FDDI Concentrator	C1	mgmt	C2/SW1	198.118.216.100	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C2	mgmt	C1/SW1	198.118.216.101	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C3	mgmt	C4/SW4	198.118.214.102	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C4	mgmt	C3/SW4	198.118.214.4	198.118.214.0	255.255.255.0	198.118.214.255	198.118.214.2
FDDI Concentrator	C5	mgmt	C6/C7/SW2	198.118.214.5	198.118.214.0	255.255.255.0	198.118.214.255	198.118.214.2
FDDI Concentrator	C6	mgmt	C5/C7/SW2	198.118.216.103	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C7	mgmt	C5/C6/SW2	198.118.216.104	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C8	mgmt	C9/SW3	198.118.216.105	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
FDDI Concentrator	C9	mgmt	C8/SW3	198.118.216.106	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
Ethernet Hub	E1	mgmt	C5/C6/C7/SW2	198.118.216.109	198.118.224.64	255.255.255.0	198.118.216.255	n/a
FDDI Switch/Router	FDDI Switch/Router							
		fddi 1,2,3	Planning & Data Proc FDDI	198.118.216.97	198.118.216.0	255.255.255.0	198.118.216.255	n/a
		fddi 4	Ingest FDDI	198.118.214.2	198.118.214.0	255.255.255.240	128.161.7.31	n/a
		fddi 5	EBNet Router	198.118.223.53	198.118.223.52	255.255.255.252	198.118.203.55	n/a
		fddi 6	Direct Attached Router	148.165.22.10	146.165.22.0	255.255.255.0	146.165.22.255	n/a
		fddi 7	ISOLAN	192.94.65.15	192.94.65.0	255.255.255.0	192.94.65.255	n/a
		fddi 8	M&O Network	198.119.143.1	198.119.143.0	255.255.255.0	198.119.143.255	n/a

Table 6. LaRC DAAC Pre-Release B Testbed IP Address Assignments for Network Hosts

Hardware Descriptor	Designator (diagram)	Port	Host Name	Concentrator or Hub ID	IP Address	Network Address	Network Mask	Broadcast Address	Default Route
ACMHW	LARC-4	NFS Server	aclml4sgi	C6 & C7	198.118.216.134	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
ACMHW	LARC-5	Workstation	acml5sun	C5	198.118.216.153	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
AITHW	LARC-1	AIT WS	plnl1sun	C1	198.118.216.110	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
AITHW	LARC-2	AIT WS/DBMS Server	plnl2sun	C1 & C2	198.118.216.111	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
AITHW	LARC-3	HP Laser Printer	aitl3hp	E1	198.118.216.112	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
CSSHW	LARC-1	CSS Server	cssl1hp	C8 & C9	198.118.216.123	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
ICLHW	LARC-4	WS	plnl4??	C2	198.118.216.174	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
MSSHW	LARC-1	Workstation	mssl1sun	C8	198.118.216.124	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
MSSHW	LARC-2	HP Laser Printer	mssl2hp	E1	198.118.216.125	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
MSSHW	LARC-3	MSS Server	mssl3hp	C8 & C9	198.118.216.126	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
MSSHW	LARC-4	MSS Server	mssl4hp	C8 & C9	198.118.216.130	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
PLNHW	LARC-1	Planning & Queuing Server	plnl1sun	C1 & C2	198.118.216.114	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
PLNHW	LARC-2	Planning WS	plnl2sun	C1	198.118.216.115	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	LARC-1	Workstation	sel1sun	C9	198.118.216.163	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	LARC-12	X-Terminal	sel12ncd	E1	198.118.216.157	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	LARC-2	Workstation	sel2sun	C9	198.118.216.164	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	OAWS-2	Micron PC	sel2pc	E1	198.118.216.172	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	OAWS-3	Micron PC	sel3pc	E1	198.118.216.173	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-10	WS	sel10sun	C1	198.118.216.156	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-2	WS	sel2sun	C1	198.118.216.165	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-3	WS	sel3sun	C1	198.118.216.166	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97

Table 6. LaRC DAAC Pre-Release B Testbed IP Address Assignments for Network Hosts

SE	SPARC-4	WS	sel4sun	C1	198.118.216.167	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-5	WS	sel5sun	C2	198.118.216.168	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-6	WS	sel6sun	C2	198.118.216.169	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-7	WS	sel7sun	C2	198.118.216.170	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-8	Workstation	sel8sun	C8	198.118.216.171	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SE	SPARC-9	WS	sel9sun	C2	198.118.216.155	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-10	X-Terminal	sprl10ncd	E1	198.118.216.119	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-3	X-Terminal	sprl3ncd	E1	198.118.216.158	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-4	X-Terminal	sprl4ncd	E1	198.118.216.162	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-5	Science Processor	sprl5sgi	C1 & C2	198.118.216.120	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-6	Science Processor	sprl6sgi	C1 & C2	198.118.216.121	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-8	X-Terminal	sprl8ncd	E1	198.118.216.117	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97
SPRHW	LARC-9	X-Terminal	sprl9ncd	E1	198.118.216.118	198.118.216.0	255.255.255.0	198.118.216.255	198.118.216.97

Network Node Manager

ECS is heavily dependent on the use of computer networks and their complexity requires a comprehensive monitoring agent to assist you in network management. Hewlett-Packard OpenView (HPOV) Network Node Manager (NNM) is just such an agent. It is a multi-vendor network management tool that provides network operators and maintainers with a whole-system view for monitoring and checking the network, for quickly identifying parts of the network that may have problems, and for isolating faults on the network. It provides the following general features:

- dynamic discovery and updating of network topology including IP hosts, gateways, and networks.
- a site-wide view of network and system resources.
- status information on resources.
- event notifications and background information.
- operator interface for managing resources.

Specific monitoring capabilities (Figure 6) provided by HP OpenView include:

- a network map with color alerts to indicate problems.
- indication of network changes.
- creation of submaps for special monitoring.
- event notifications.
- User configurable thresholds.
- Access to remote terminals and remote system administration.

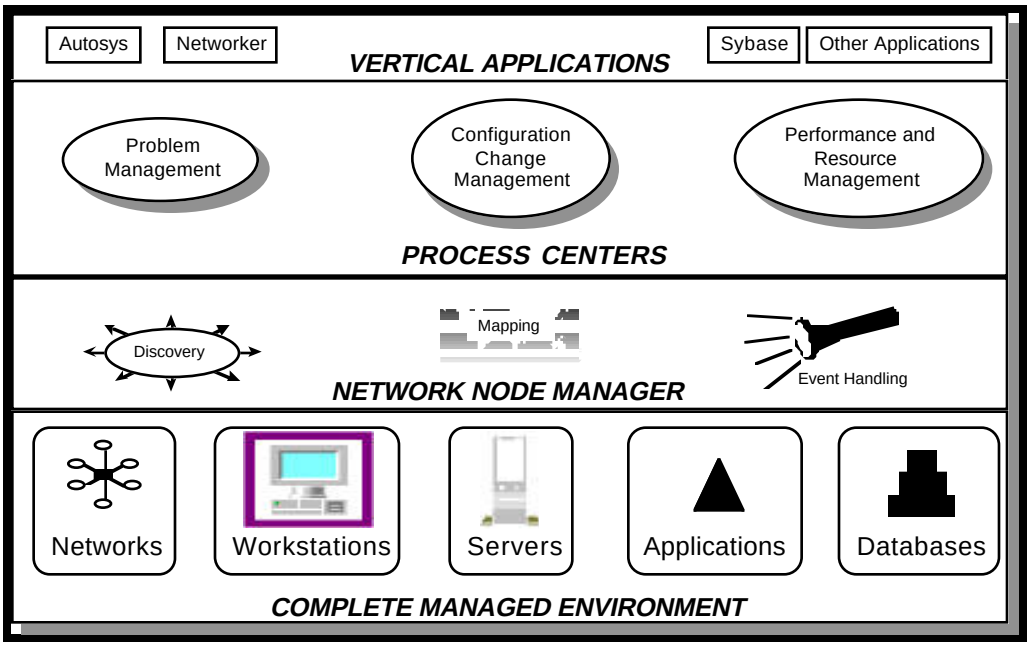

Figure 6. The OpenView Framework

Figure 7 shows a sample of a NNM map.

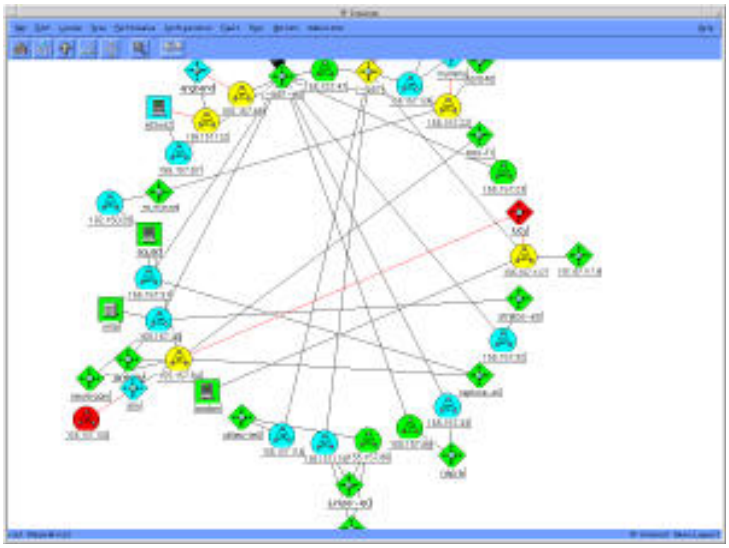

Figure 7. Sample NNM Submap

The main components of the Network Node Manager system are:

- the network monitor, the event monitor.
- the map and map database, called the Management Information Base (MIB).
- the SNMP agent process, a UNIX daemon that runs on each client machine.
- the SNMP data collection process.
- a set of network management applications.

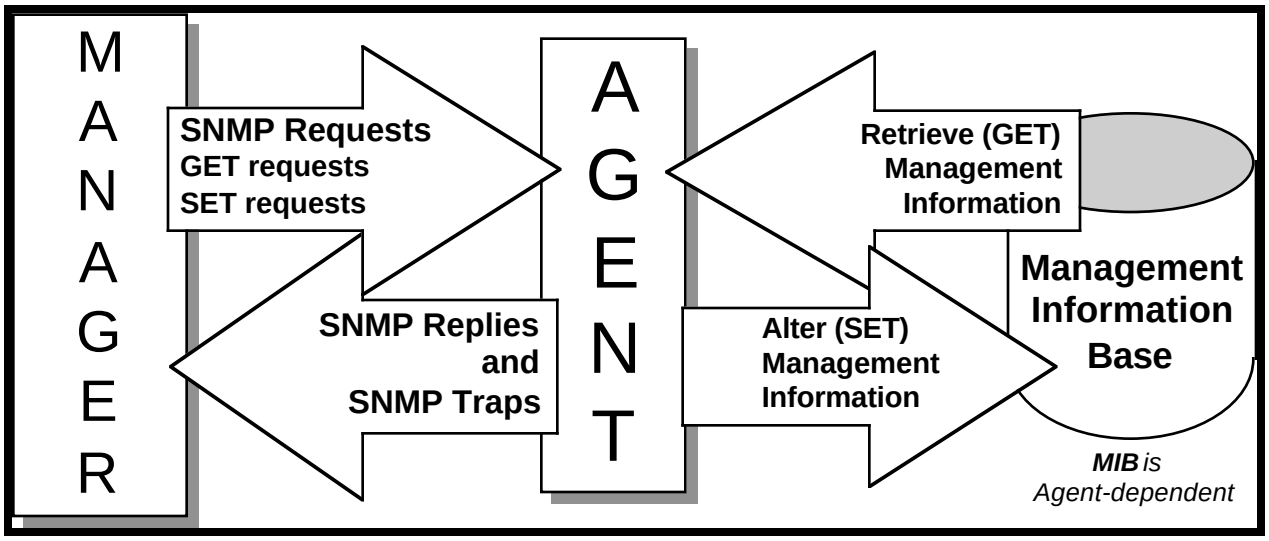

Figure 8. How Network Node Manager Works

The graphical network map is automatically drawn from network information that is discovered by the network monitor. In turn, the network monitor updates the map database whenever new topology information is discovered about the network. NNM uses the map database to generate the graphical map when it is started, then keeps the map current through events sent by the network monitor. NNM also updates the map database when editing changes are made to the map (Figure 9).

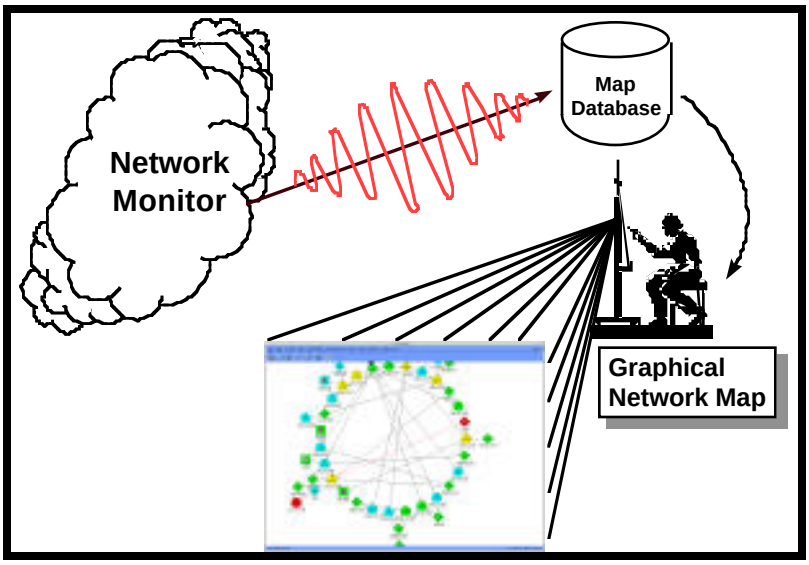

Figure 9. How the NNM Map Interface Works

Universal Pathnames

Throughout this lesson reference will be made to ***universal pathnames***. Because HPOV and NNM operate on a wide variety of operating system platforms and because each platform has its own unique file system structure, naming the full paths to particular executable files becomes impractical. Therefore, HPOV utilizes these ***universal pathnames***, a kind of UNIX shorthand, to identify the location of executables.

For example, the executable file that starts OpenView is **ovw**. On the HP-UX 9.x operating system, **ovw** is located at /usr/OV/bin/ovw while on the HP-UX 10.x operating system it is located at /opt/OV/bin/ovw. Thus, we refer to the executable as **$OV_BIN/ovw**. $OV_BIN is the shorthand referring to either /usr/OV/bin or /opt/OV/bin.

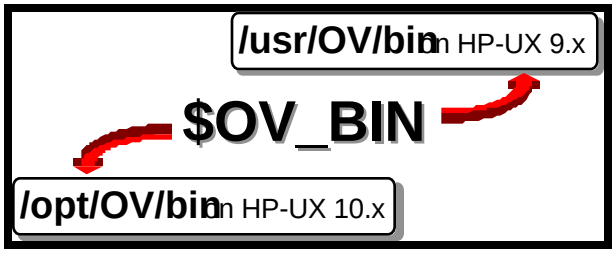

Figure 10. Universal Pathname

Starting and Ending a NNM Session

Start NNM

In order for the NNM to properly report on the network topography, HP OpenView Windows (OVW) must be activated. Once activated, OVW automatically starts NNM. OVW also automatically starts the applications that are installed and registered.

Prerequisites for this Task

The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes among others:

- **ovwdb** - The process that maintains the OVW object database.
- **trapd -** The process that multiplexes and logs SNMP traps.
- **ovtopmd** - The process that maintains the network topology database.
- **ovactiond -** The process that executes commands upon receipt of an event.
- **snmpCollect** - The process that collects MIB data and performs threshold monitoring.
- **netmon** - The process that polls SNMP agents to initially discover network topology and then detect topology, configuration, and status changes in the network.

You can check to see if these processes are running by typing **$OV_BIN/ovstatus** at a UNIX prompt.

```
object manager name: ovwdb
behavior:       OVs_WELL_BEHAVED
state:          RUNNING
PID:            174
last message:       Initialization complete.
exit status:    -

object manager name: snmpCollect
behavior:       OVs_WELL_BEHAVED
state:          RUNNING
PID:            187
last message:       Initialization complete.
exit status:    -

object manager name: ovtopmd
behavior:       OVs_WELL_BEHAVED
```

Figure 11. Sample Output of* ovstatus *Command

Start the HP OpenView Windows Graphical User Interface Procedure

1 If X Windows are not already running, at the command line type **x11start** at the command prompt and **press enter**.

- This command will start the X Windows session.

2 Type **ovstatus** at the UNIX command prompt, then press **Return**.

- This command checks the status of the processes.
- If the network management processes are not running, type **$OV_BIN/ovstart** at the UNIX command prompt, then press **Return**.

3 Type **$OV_BIN/ovw &** at the command prompt, then press **Return**.

- If the **$OV_BIN** directory is in your path, type **ovw &** to start HP OpenView Windows.
- OVW displays the **About OVW** dialog box. After a few moments, you see the OVW Windows home submap.

Exit HP OpenView Network Node Manager Session

To exit NNM and all other integrated applications, you must exit OVW in one of the following two ways (Figure 12):

Exit NNM Procedures

---

1 From the menu bar on any submap window, select **Map**, then select **Exit**; ***or***

2 Click on the **Close** button on all open submap windows until a warning dialog box is displayed. Then click on the **Close** button to exit OVW.

> ***WARNING: Do not use the CLOSE WINDOW button in the upper left corner of the window to exit OVW. This may cause some OVW processes to remain in operation and could result in system-wide problems later.***

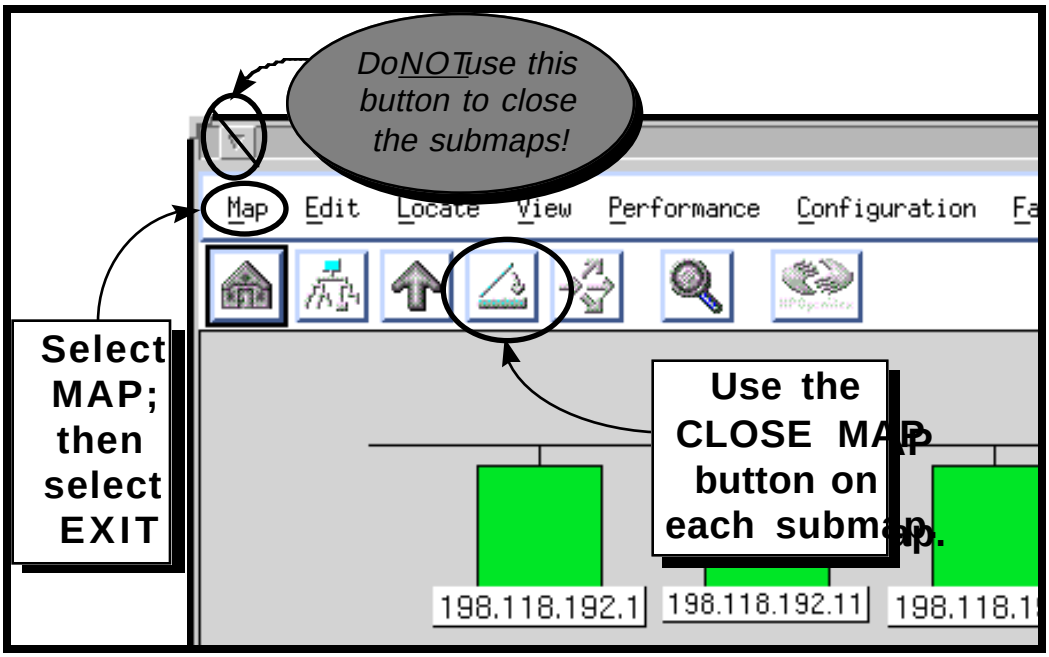

Figure 12. End an NNM Session

This page intentionally left blank.

The NNM Map and Submaps

The NNM Map is never seen in its entirety. What you observe when using NNM is a set of submaps that allow you to view specific portions of the map as you to track network activity. This is similar in concept to the way that you rarely view a complete map of the world; rather you view specific portions of that map (Figure 13).

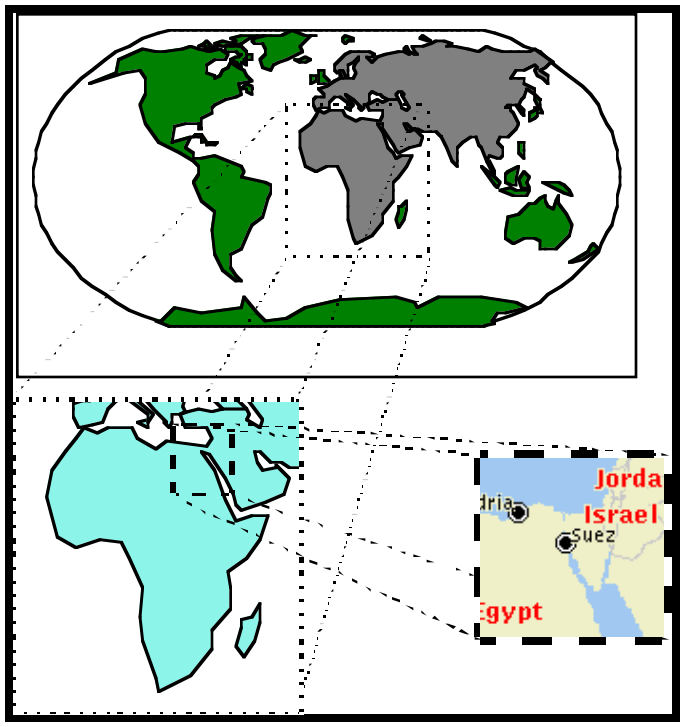

Figure 13. Demonstrating the Concept of a Map and Submaps

A **MAP** is:

- A set of related objects, symbols, and submaps.
- A collection of submaps.
- Represents topology and state or real-world network.

A **SUBMAP** is:

- A collection of related symbols.
- Represents a view of the network.
- Part of the hierarchical structure (Figure 14).

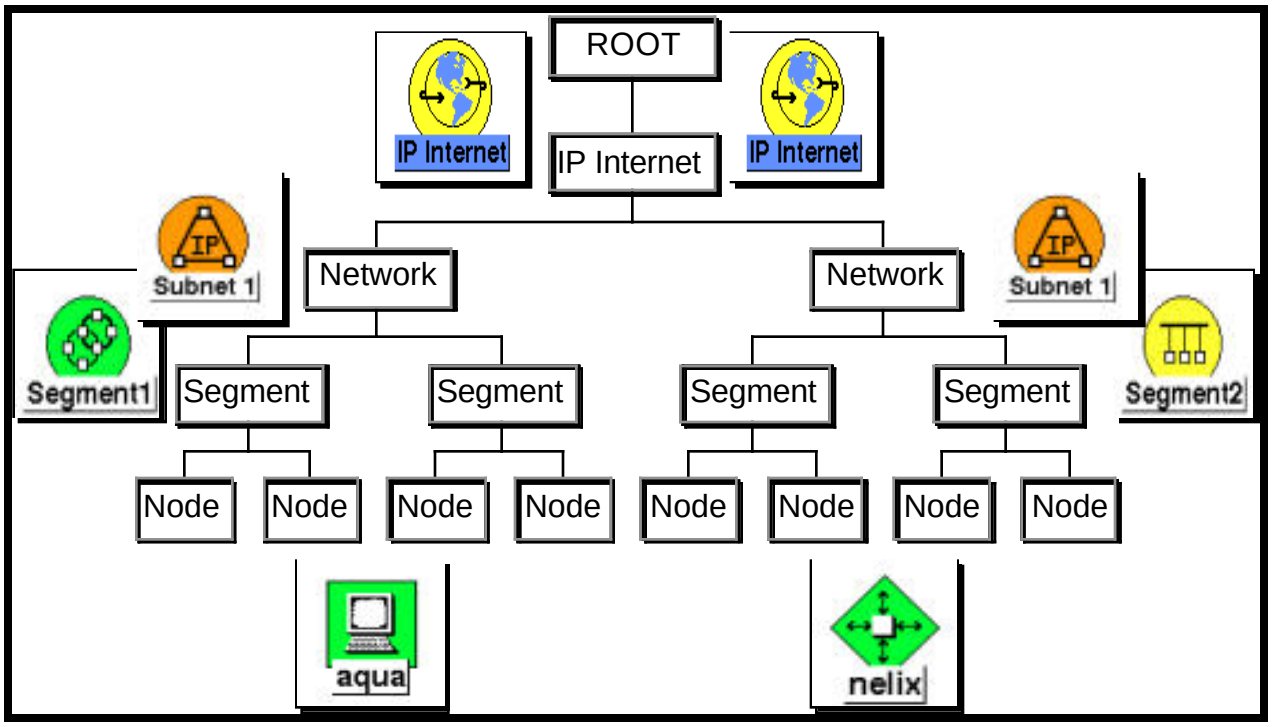

Figure 14. Submap Hierarchical Structure

As shown, there are four parts to each submap:

- Menu Bar
- Tool Bar
- Viewing Area
- Status Line

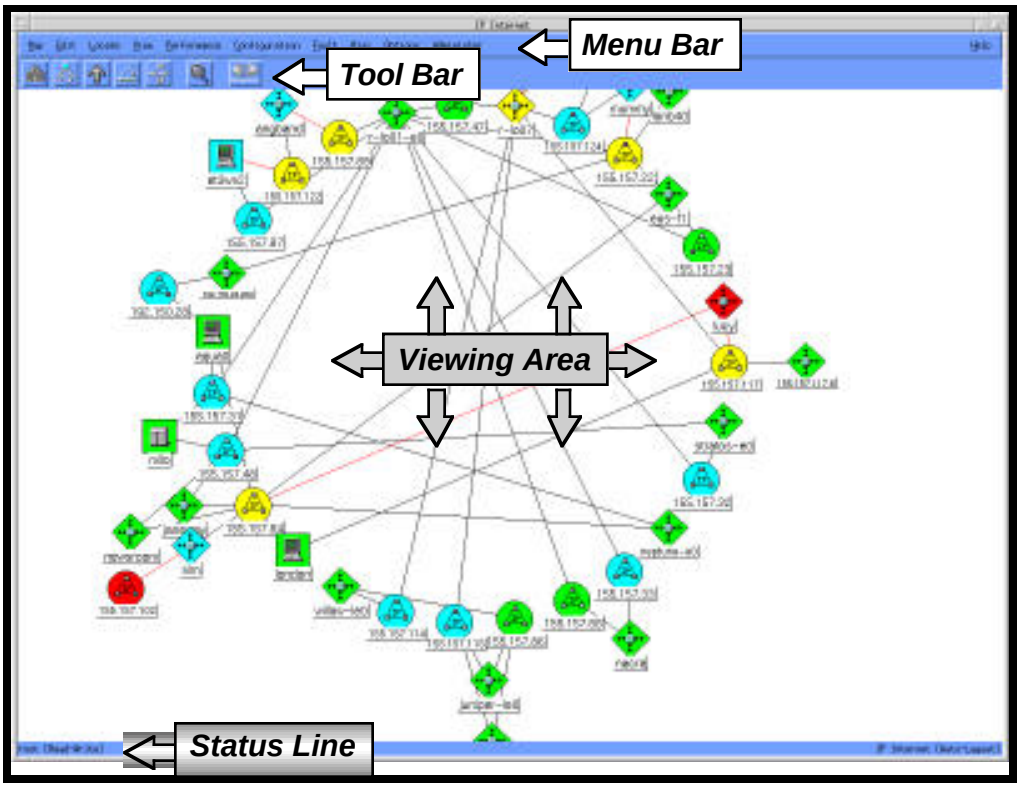

Figure 15. Parts of a Submap

Menu Bar

The **Menu Bar** offers a set of choices for performing a variety of tasks such as creating new maps and submaps, creating and modifying object information, and configuring thresholds.

Tool Bar

The **Tool Bar** (Figure 15) is used to quickly maneuver through the graphical displays. The Tool Bar has several special buttons that perform a variety of routine tasks.

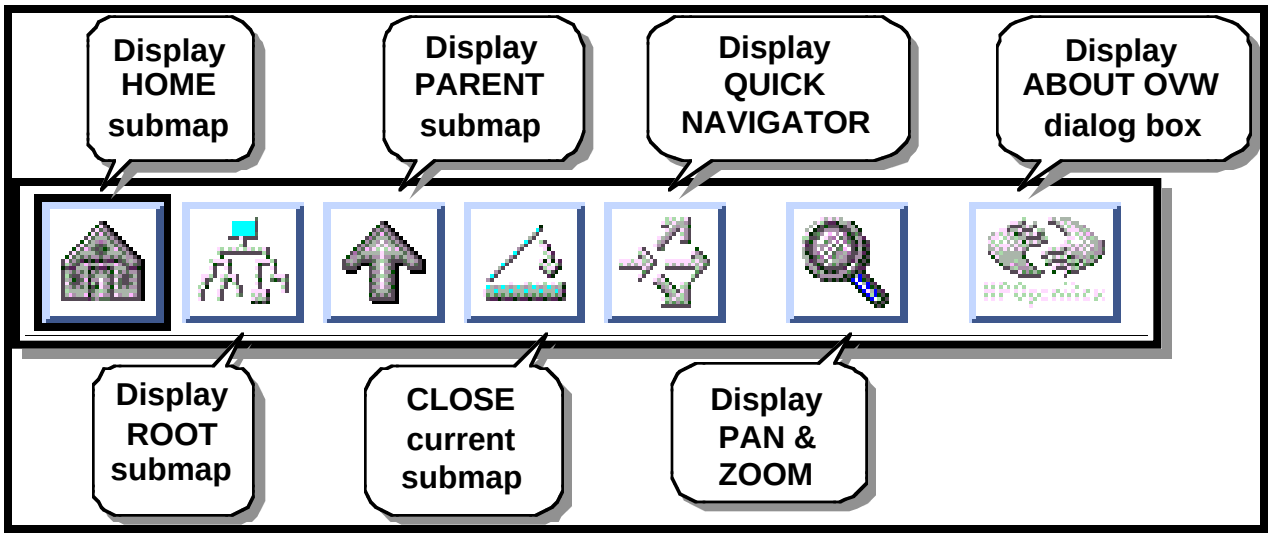

Figure 16. Sample Tool Bar

HOME button – When NNM starts up, you are placed in a particular submap by default. This default submap is called the **home** submap. Any submap can be so identified. When the **Home** button is selected, the display returns your particular home submap.

ROOT button – Displays the **root** submap.

PARENT button – Displays the **parent** submap to the current submap.

CLOSE button – Closes the current submap. Use this button to back your way out of NNM. This performs the same procedure as selecting **Map** → **Close Submap** from the pull-down menu.

QUICK NAVIGATOR button – Allows you to move from one submap to another without moving explicitly through the hierarchy. Using the Menu selection **Edit** → **Add to Quick Navigator**, you can select specific submaps or symbols that you monitor on a regular basis.

PANNER button – Some submaps are so extensive that the entire submap view cannot be seen. Using this panner allows you to shift the view of a particularly large submap so that you can zoom in on a desired area of a submap.

ABOUT OVW DIALOG button – Displays the OVW dialog box.

Viewing Area

The **Viewing Area** is your window into the submap being currently displayed. By default, the entire submap is shown within the viewing area. On sum complex maps you may wish to use the **Pan and Zoom** feature to zero in on a specific area.

Status Line

Messages on the status line indicate the status of OVW including:

- the name of the open map.
- Read-Write access permissions.
- name of the open submap.
- status of the auto-layout feature (on or off).

Other messages may appear on the Status Line from time to time, such as **synchronizing**, which indicates that the map is being updated with the latest information in the MIB.

This page intentionally left blank.

Network Objects and Symbols

Objects

Objects represent logical or physical entities or resources that exist in a network environment. An object usually represents something of interest, like:

- another network.
- a LAN segment.
- a particular Ethernet cable or RS-232 line.
- another software interface on a workstation.
- a software application running on a computer.
- a process running on a computer.
- a logical IP connection of a gateway to a network.

Each object is uniquely identified by a **selection name** and is further defined by a variety of attributes.

Symbols

A symbol is a graphical representation of an object on a submap. There are a large number of symbols categorized by the type of object they represent.

Before adding a new object to the NNM you should have information on these:

- hostname.
- IP Address.
- IP status.
- description.
- owner.

Add a Network Object Procedure

Prerequisite: NNM is running and the IP submap onto which the new object will be attached is open with both read and write permissions.

1 Type **ovstatus** at the UNIX command prompt, then press **Return**.

- This command checks the status of the processes.
- If the network management processes are not running, type **$OV_BIN/ovstart** at the UNIX command prompt, then press **Return**.

2 Type **$OV_BIN/ovw &** at the command prompt, then press **Return**.

- If the **$OV_BIN** directory is in your path, type **ovw &** to start HP OpenView Windows.
- OVW displays the **About OVW** dialog box. After a few moments, you see the OVW Windows home submap.

3 Select **Edit: Add object**

- The **symbol palette** appears displaying a variety of symbols (Figure 17).

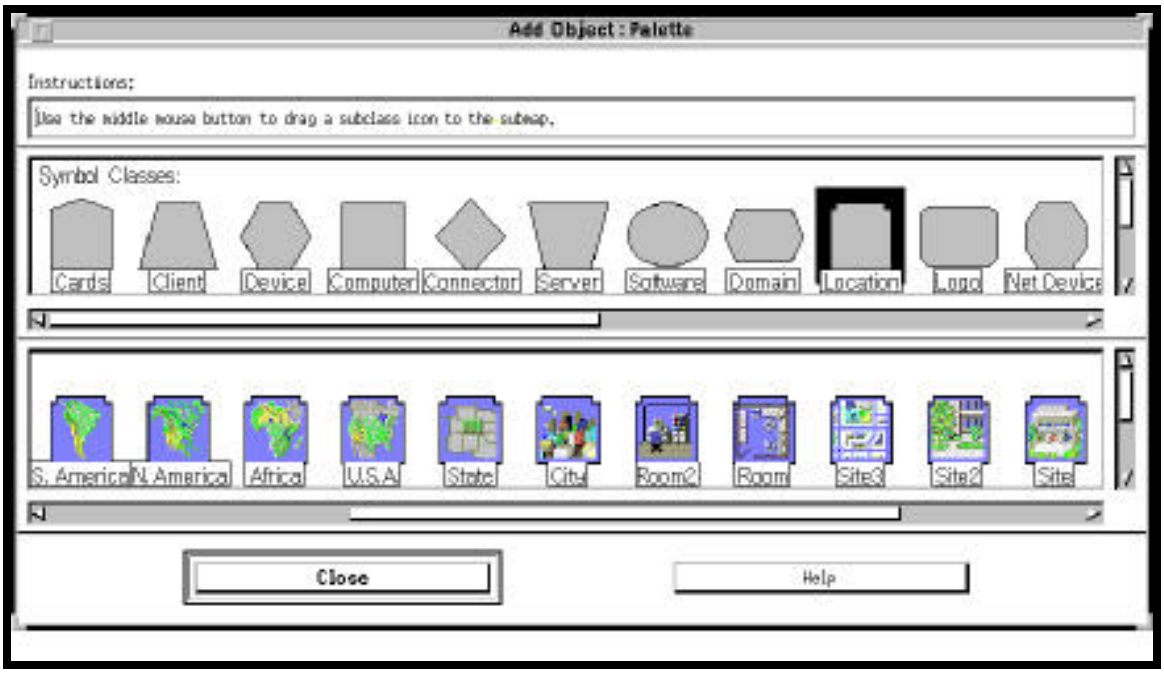

Figure 17. Add Object Palette

1 From the symbol palette, choose the desired symbol type for the network object by selecting the desired subclass and use button 2 to drag the symbol to the submap. The **Add object** dialog box appears.

2 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

3 In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a network object appears.

4 Enter a **Network Name.**

5 Enter a **Network Address**.

- Optionally, **Network Subnet Mask** can be entered.

6 Click **Verify** to check for valid entries.

7 Click on **OK** to close the **Set Attributes** dialog box.

8 Click on **OK** in the **Add Object** dialog box to complete the operation.

This page intentionally left blank.

Adding a Segment Object

A **segment submap** represents the physical topology of a segment of the network at the level of nodes and connectors (Figure 18).

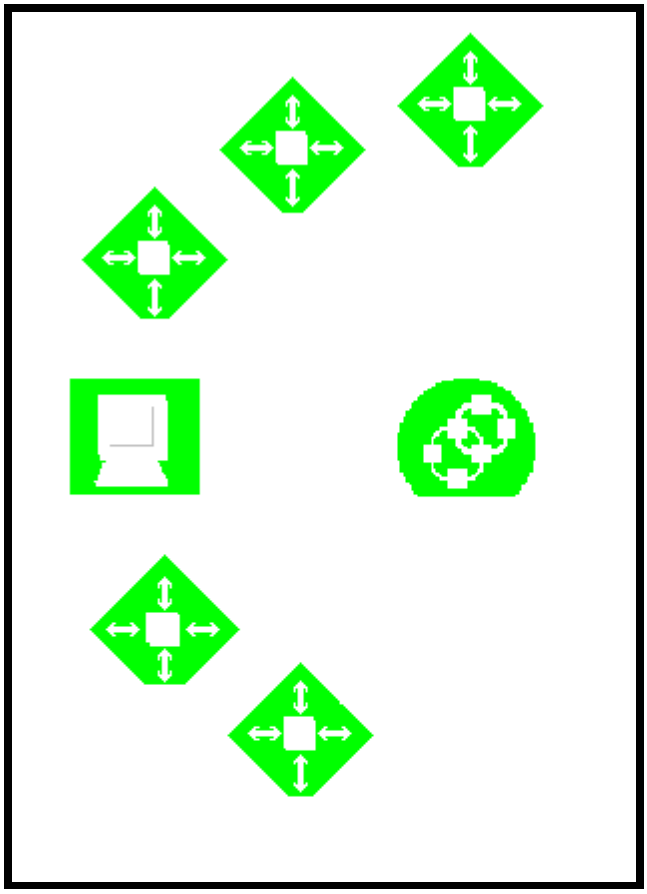

Figure 18. Segment Submap

Nodes belonging to the same segment typically use a common physical medium to communicate with each other, e.g., Ethernet, Token Ring, phone lines, satellite links.

During discovery of a network, if the IP Map can identify which segment the node is on, it places it there. If the IP Map cannot identify which segment the node is on, it place the segment on the default segment submap.

The default segment submap is the submap created by IP Map when OVW was first started. If that submap has been deleted, the default segment submap becomes the oldest segment submap. IP

Map discovers new nodes on segments attached to SNMP, IP addressable bridges, and multiport repeaters (hubs).

Add a Segment Object Procedure

Prerequisite: NNM is running and the IP map onto which the new object will be attached is opened with read and write permissions.

1 Select **Edit** → **Add Object**.

2 From the symbol palette, choose the desired symbol type for the segment object by selecting the desired class, then the desired subclass, and drag the symbol to the submap using the middle mouse button. The **Add Object** dialog box appears.

3 Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.

4 In the **Object Attributes** list, select **IP Map** and click **Set Object Attributes**. The **IP Map Set Attributes** dialog box for a segment object appears. A figure of the dialog box follows this procedure.

5 Enter a **name for the segment**. It must be unique to other segment names in the submap.

6 Click **Verify** to check for valid entries.

7 Click on **OK** to close the **Set Attributes** dialog box.

8 Click on **OK** in the **Add Object** dialog box to complete the operation.

Adding an IP Interface Object

Adding an IP Interface Object

You can add an IP interface to a Node submap by placing an IP Interface symbol on a Node submap. This is done by entering the IP address of the interface.

Add IP Interface Object Procedure

Prerequisite: NNM is running and the IP submap onto which the new object will be attached is open with both read and write permissions.

1 Select **Edit** → **Add Object** from the resulting menu.

- The symbol palette appears. In the **Class** upper window, click on **Cards** to display the appropriate subclass symbols in the lower window; then click on the **IP Interface** symbol. The **Add Object** dialog box opens.

2 In the **Selection Name** field, enter a unique selection name.

3 In the **Object Attributes** list, select **IP Map**, then click **Set Object Attributes**.

- The IP Map **Set Attributes** dialog box for an IP interface object appears (Figure 19).

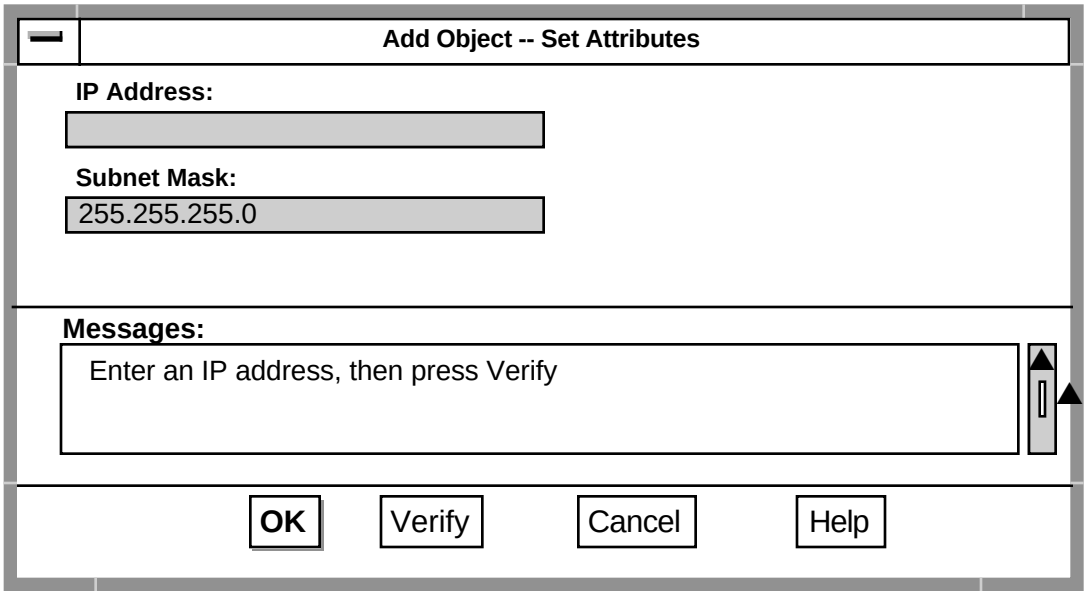

Figure 19. Add IP Interface Object Screen

4 In the **IP Address:** field, enter the IP address for the IP interface

- The subnet mask is automatically added in the **Subnet Mask:** field.

5 Click on the **Verify** button at the bottom of the window to check for valid entries.

6 Click on the **OK** button at the bottom of the window to close window.

7 Click on the **OK** button in the **Add Object** dialog box to complete the operation.

Viewing Current Network and System Configuration

Viewing Current Network and System Configuration

NNM provides quick access to information about your network and system configurations. This section points you to the menu items available to accessing this information.

View Current Network and System Configuration Procedure

Prerequisite: NNM is running and a submap is open with at least read permission.

1 Select one or more nodes from the map. If more than one node is selected a dialog box for each selected node will be displayed.

- To select more than one node from the map, click on the first symbol to select it. Then hold the **CTRL** key while clicking the next symbol to select it. Repeat this procedure until all desired symbols have been selected.

2 Select the object for which a description is desired. The object may be:

- an IP Internet Object
- a Network Object
- a Segment Object
- a Node Object
- an Interface Object

3 From the menu bar, select **Monitor**; then select **Description-Selected Objects** from the resulting menu. The **Object Description** dialog box is displayed (Figure 20).

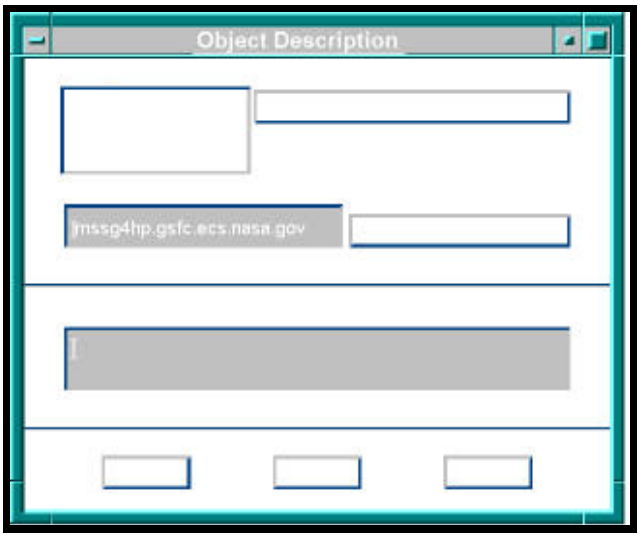

Figure 20. Object Description Dialog Box

4 In the **Object Description** dialog box, select **IP Map**; then select **View/Modify Object Attributes**. An **Attributes** dialog box (Figure 21) for each type of object selected in Step 2 appears.

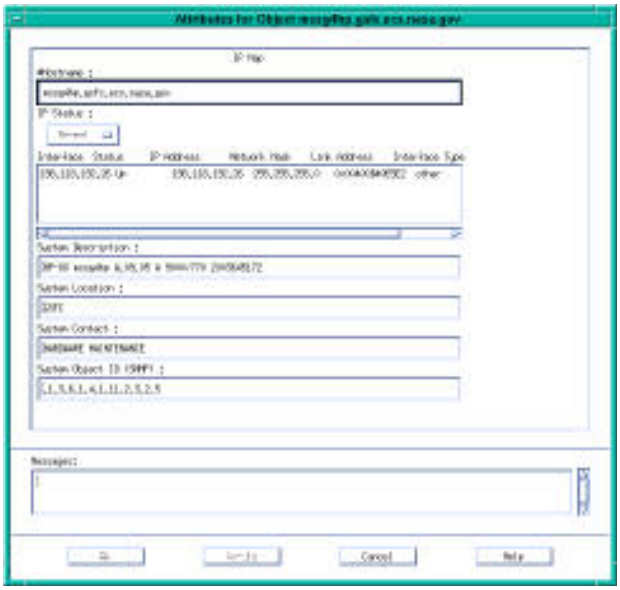

Figure 21. Object Attributes Dialog Box

5 After viewing the configuration data for each selected object, click the **Cancel** button to close the window.

Viewing Network Address Information

This task is useful for determining the addresses associated with a node without looking through configuration files. The information displayed is real-time data taken from the node as opposed to static information taken from a database; that is, the data you see is what is currently occurring on the system (Figure 22).

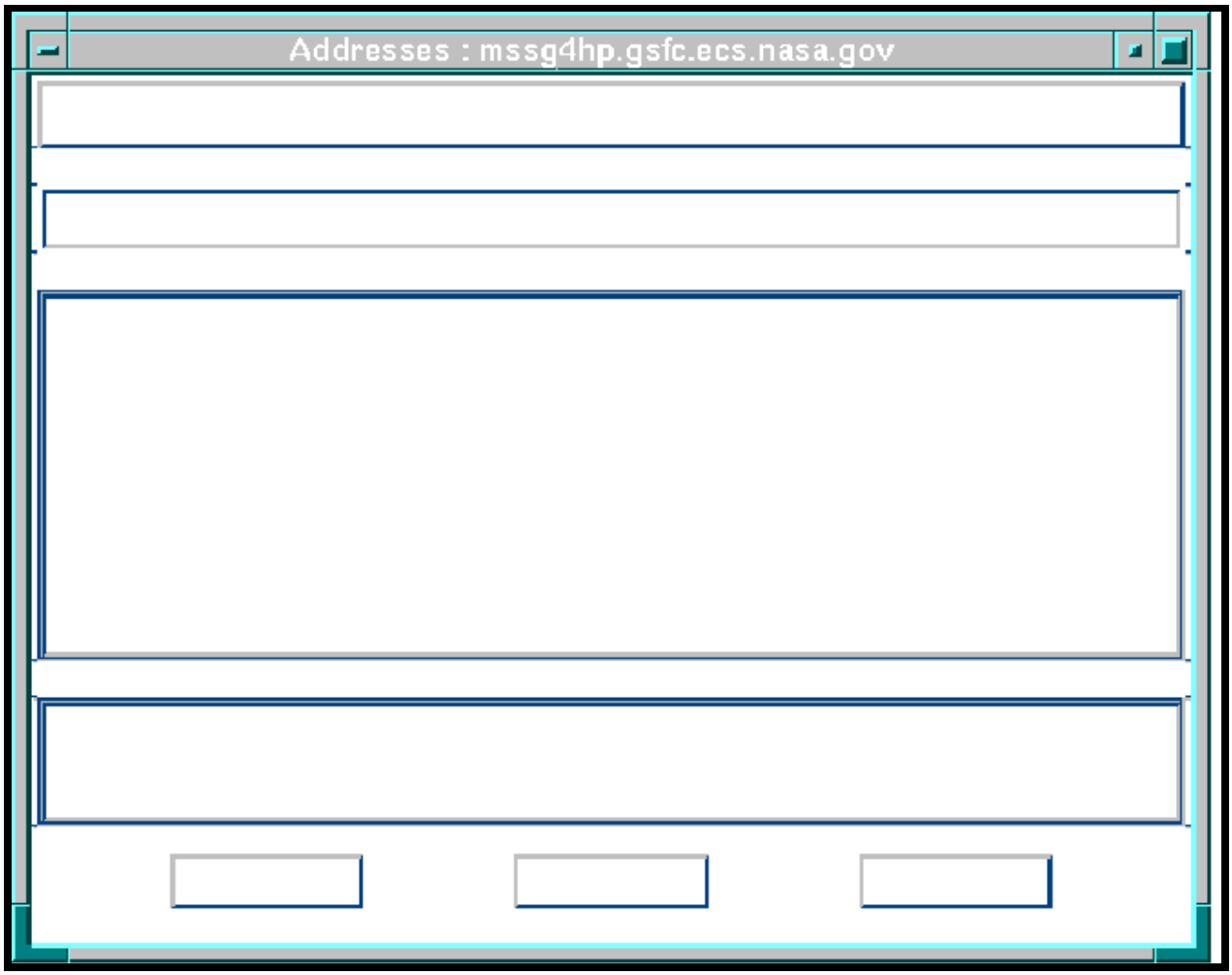

Figure 22. Viewing Network Address Information

Viewing Network Address Information Procedure

Prerequisite: NNM is running and a submap is open with at least read permission.

1 Select one or more nodes from the map. If more than one node is selected a dialog box for each selected node will be displayed.

- Be sure the node(s) you are about to select support(s) SNMP.
- To select more than one node from the map, click on the first symbol to select it. Then hold the **CTRL** key while clicking the next symbol to select it. Repeat this procedure until all desired symbols have been selected.

2 From the menu bar, select **Monitor**; from the resulting menu select **Network Configuration** → **Addresses** to view the following information about each interface:

- interface index
- interface name
- IP address
- network mask
- network address
- link-level address (physical address)

3 After viewing the configuration data for each selected object, click the **Close** button to close the window

Viewing How Traffic is Routed on a Network

This task lists the routing table information for a remote SNMP node (Figure 23). It can be useful in determining more efficient routes on the network, assessing the need for explicit routes and diagnosing connectivity problems. The information you see is real-time data taken from the node.

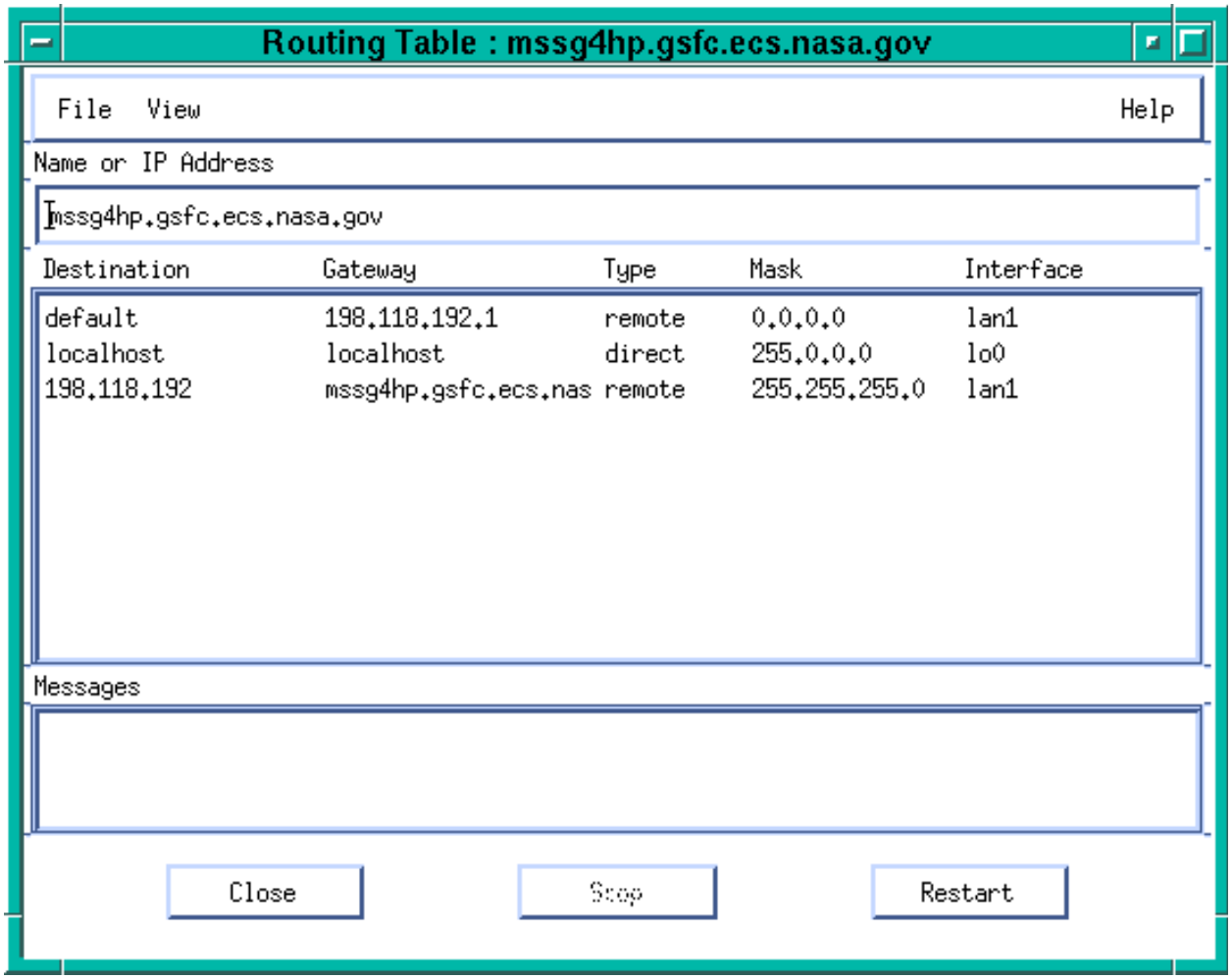

Figure 23. Viewing How Traffic is Routed Through the Network

Viewing Network Traffic Routing Procedure

Prerequisite: NNM is running and a submap is open with at least read permission.

1 Select one or more nodes from the map. If more than one node is selected a dialog box for each selected node will be displayed.

- To select more than one node from the map, click on the first symbol to select it. Then hold the **CTRL** key while clicking the next symbol to select it. Repeat this procedure until all desired symbols have been selected.

2 From the menu bar select **Monitor**. From the resulting menu select **Network Configuration** → **Routing Table**. The following information will be displayed:

- destination name (**default** is a route that the system uses when it cannot find a specific route.
- name of the gateway (router) between selected node and destination.
- type of route (e.g., directly connected to a LAN, through a remote gateway, or route not currently available).
- network subnet mask associated with the route.
- name of the interface that is used to reach the destination.

3 When you are finished reading the data, click the **Close** button to close the window.

Viewing the Services Available on a Node

This task lists the IP networking services for which a remote SNMP node is listening. It is useful for determining what configured services a node is currently running. The information you see is real-time data taken from the node (Figure 24).

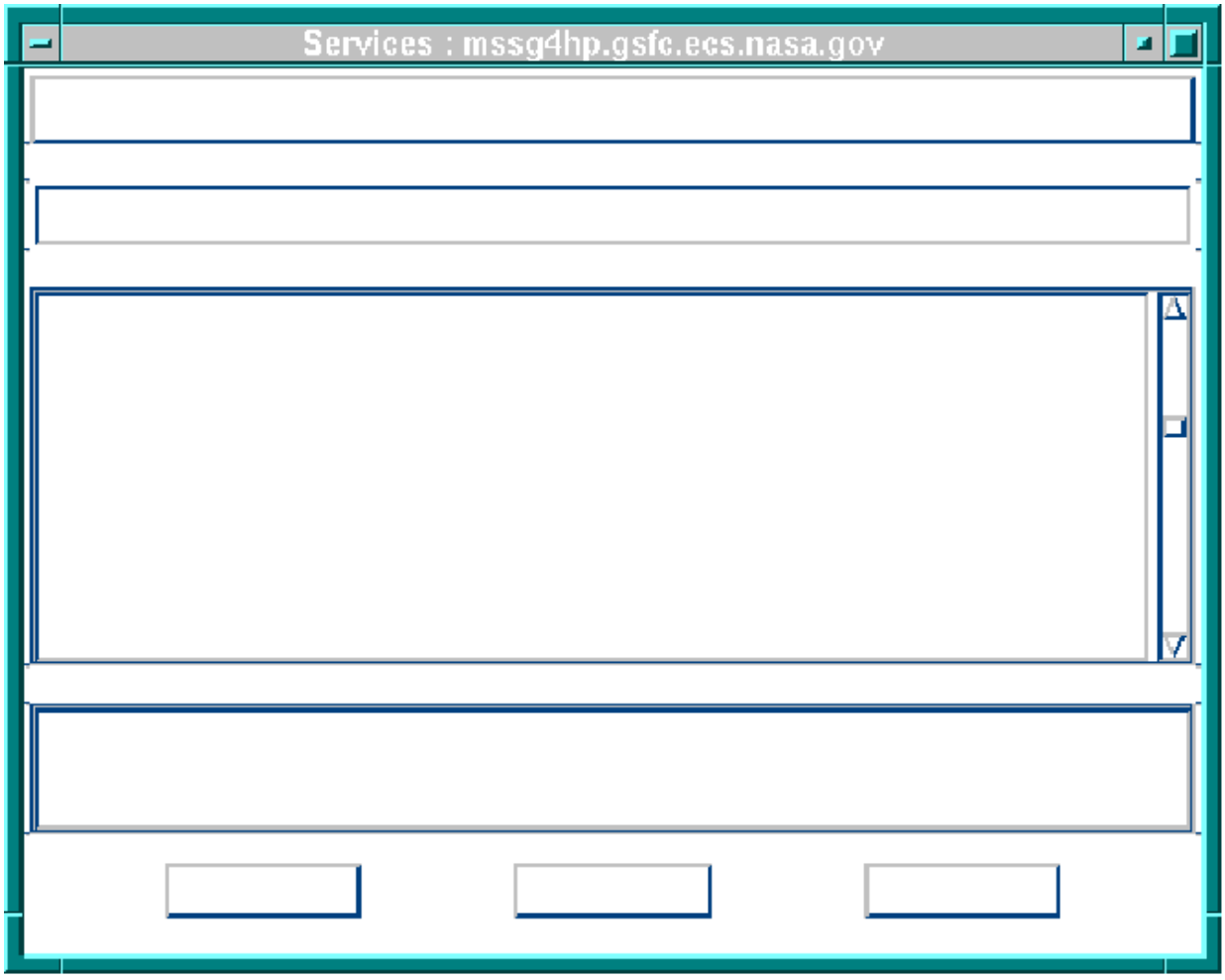

Figure 24. Viewing Available Services on a Network Node

Viewing Available Services Procedure

Prerequisite: NNM is running and a submap is open with at least read permission.

1 Select one or more nodes from the map. If more than one node is selected a dialog box for each selected node will be displayed.

- To select more than one node from the map, click on the first symbol to select it. Then hold the **CTRL** key while clicking the next symbol to select it. Repeat this procedure until all desired symbols have been selected.

2 From the menu bar select **Monitor**; from the resulting menu select **Network Configuration** → **Services**. The following information is displayed:

- The service protocol, either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
- the port to which the service is bound.
- The service for which the node is listening (e.g., telnet, nfs). If no service is listed, the service is either unavailable or unknown.

3 When you are finished reading the data, click the **Close** button to close the window.

System Monitoring

Once a network has been discovered by HP OpenView discovery and layout, monitoring the state of the network can begin. Monitoring includes such tasks as:

- checking the map for color alerts which indicate problems.
- creating submaps needing special monitoring.
- checking for network changes.

Looking at Maps for Color Alerts

HP OpenView uses colored symbols to indicate the health and operational status of the various objects within the network. These status states are divided into **Operational** and **Administrative** categories.

Operational Status

Operational status refers to the actual operation of the node on the submap. Operational status is changed by NNM automatically when a change in the operational condition of the node is detected. Table 7 below describes the various operational status colors and conditions:

Table 7. Operational Status Colors

Symbol Color	Status
Blue	UNKNOWN. A device or a network that has not been discovered by NNM. This can happen when a non-IP addressable device has been added to the map manually and NNM has not yet discovered it. The status is set to Unknown; it cannot be determined.
Green	NORMAL. The device or network is up and functioning normally. The object is in its Normal operational state.
Cyan	WARNING. There is a potential fault or problem
Yellow	MINOR or MARGINAL. There is something wrong with this object, but the device is still responding to NNM.
Orange	MAJOR. This object is in a state of having a Major fault or problem.
Red	CRITICAL or DOWN. The device is not responding to NNM.

Administrative Status

Administrative status refers to the administrative function that is occurring on the node. Administrative status is changed by the Fault Manager. Table 8 describes the various administrative status colors and conditions:

Table 8. Administrative Status Colors

Symbol Color	Status
Off-white	UNMANAGED or UNMONITORED. The status information on this object is not maintained.
Salmon	TESTING. The object is undergoing some form of diagnostic procedures.
Tan	RESTRICTED. The object is set for restricted or dedicated usage.
Dark Brown	DISABLED. The object is operationally disabled or inactive.

Compound Status

When a symbol changes color, either the node itself has incurred a problem or a node within the segment has experienced trouble. This is known as **Compound Status**. The compound status of a symbol is a configurable option, allowing the network manager to set thresholds as to when the symbol will change color and how many levels through the submaps the color changes will occur. When the symbol changes color, the network manager must trace, or drill down, through the submaps to determine where the problem has occurred.

Propagate Status

The **Propagate Status** is the level at which changes in the appearance of the symbols on the submaps occur. There are three levels of propagate status that can be set:

- **Default status**—depending on the operational or administrative status of symbols in child submaps, the color of the parent object will change. Table 9 below describes the various scenarios:

Table 9. Default Status Propagation

Condition of Symbols on Child Submap	Status of Symbols on Parent Object
No symbols are normal and no symbols are abnormal	Unknown
All symbols are normal	Normal
One symbol is abnormal; all other symbols are normal	Warning
More than one symbol is abnormal and more than one other symbol is normal	Minor/Marginal
One symbol is normal; all other symbols are abnormal	Major
All symbols are abnormal.	Critical

- **Propagate Most Critical status** – the most critical symbol on a child submap is displayed on the parent object. Table 10 demonstrates a few scenarios of this type of status display:

Table 10. Propagate Most Critical Status

Condition of Symbols on Child Submap	Status of Symbols on Parent Object
No symbols are normal and no symbols are abnormal	Unknown
All symbols are normal	Normal
One symbol is critical, all other symbols are normal	Critical
One symbol is critical, all other symbols are major	Critical
One symbol is marginal, two symbols are warning, others normal	Marginal

- **Propagate at Threshold Value (0-100%)** – the color of the parent object changes when a minimum percentage of symbols on a child submap have changed color. If more than one status state is detected, the most severe status is propagated. In addition, a pop-up notice may be programmed as well (Figure 25).

Figure 25. Threshold Event Pop-Up Notification

Table 11 describes the default threshold values that can be edited:

Table 11. Propagate at Threshold Value (0-100%)

Change the Compound Status of the Parent to:	When this percentage have changed:
Warning	30
Minor	20
Major	10
Critical	5

To interpret the meaning of status colors correctly, the compound status scheme of the open map should be known. This tells how status propagates from objects in a submap to the parent object. The compound status scheme for the map from the **Map Description** dialog box can be identified by selecting **File: Describe/Modify Map.**

The following procedure follows the rules for Default propagation and assumes that an abnormal condition exists that has caused a node on the network to propagate a minor or marginal problem. This procedure can be used to trace through the network to isolate the problem.

Looking at Maps for Color Alerts Procedure (Default Propagation)

---

1 Double click on the yellow **Internet IP** symbol.

- The **Internet submap** opens and displays three IP networks attached to two gateways. One IP network symbol is yellow. This indicates a marginal problem with the network.

2 Double click on the yellow **IP network** symbol.

- A **Network submap** opens and displays three segments attached to two gateways. One segment symbol is yellow. This indicates a problem somewhere on the segment.

3 Double click on the yellow **segment** symbol.

- A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.

4 Double click on the red **workstation** symbol.

- A **Node submap** opens and displays two interface symbols, which indicate that two interfaces are installed on the workstation. One of them is red.
- You have isolated the fault to a single card of a single node on your internet.

Checking the Health and Status of the Network

Objects that have an abnormal condition can be identified without having to look at every symbol on the network submap. A color alert on a symbol indicates that some part of that object may have problems. To isolate a fault somewhere on the network, follow the color alerts to increasingly more specific submaps until the specific object that is not functioning is reached. Follow color alerts by opening child submaps of objects that contain a color alert.

Verify That an Object Is Not Functioning

This section explains how to verify that an object is not functioning and assumes that HP OpenView is running on the desktop. To verify that an object is not functioning, any of the following procedures may be executed.

Verify Object Not Functioning Procedures

1 Select the **Monitor** pull down menu

2 Select **Device Configuration**

3 Select **System Information**

-or-

1 Select the **Diagnose** pull down menu

2 Select **Network Connectivity**

3 Select **Demand Poll**

-or-

1 Select the **Diagnose** pull down menu

2 Select **Network Connectivity**

3 Select **Ping**

If these operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network.

Looking at Maps for New Nodes

Because discovery is automated, new objects on the network will be added automatically to the map when they are discovered. In order for this to happen, the **IP Map** must be enabled for the map, which it is by default. **IP Map** places new symbols directly on the submap if **autolayout** is enabled. IP Map places new symbols in the **New Object Holding Area** if **autolayout** is disabled for the submap.

Looking at Maps for New Nodes Procedure

1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.

- View the submap for any new symbols.

2 To easily see new symbols in the submap, disable **autolayout** for the submap.

- All newly added symbols are placed in the **New Object Holding Area**.
- When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.

Creating Special Submaps for Monitoring Status

IMPORTANT: See section 4-5 of the *HP OpenView Network Node Manager User's Guide* to use this feature.

Creating Special Submaps for Monitoring Status Procedure

1 Decide where to locate your submap and whether it will have a parent or not.

- A submap without a parent object is independent of other existing submap hierarchies in the open map, and can be opened only from the **Available Submaps** dialog box. You can create child submaps of this submap, thereby creating a new submap hierarchy in the map.
- A submap that has a parent object can be opened from an explodable symbol of the parent object. If you want the new submap to exist within an existing submap hierarchy, you should create this submap from an explodable symbol.

2 To create a submap within an existing hierarchy, decide which symbol to use to open the new submap.

- If other symbols on the parent submap already open into child submaps or execute applications, you must create a new symbol to open the submap.
- If you decide to create a new symbol (as in this case), add a symbol (for an existing object – in this case, a gateway) or a new symbol and object to the submap of your choice (in this case, the Internet submap), following menu path **Edit** → **Add Object . . .**

3 You may add either of the IP Internet symbols or any of the symbols in the location class.

4 Open the new submap by double-clicking on the newly created symbol. Copy gateway objects from other submaps into the newly created map, following menu path **Edit** → **Copy and Edit** → **Paste** operations.

5 For more information about these operations, see the *HP OpenView Windows User's Guide*.

Checking for Event Notifications

Whenever a change occurs on the network, an **event** is generated. The occurrence of the event has two consequences:

- Through the internal processors of the **Network Node Manager**, the event is registered in a predefined category for display in an **Events Browser** window (Figure 26).

- The registration in the Events Browser window triggers a change for display in an **Event Categories** window (Figure 27) to provide a notification that an event has occurred in the category of that Events Browser window. The display is a color change in a button on the Event Categories window corresponding to the event category. The color of the button indicates the highest severity event in the category.

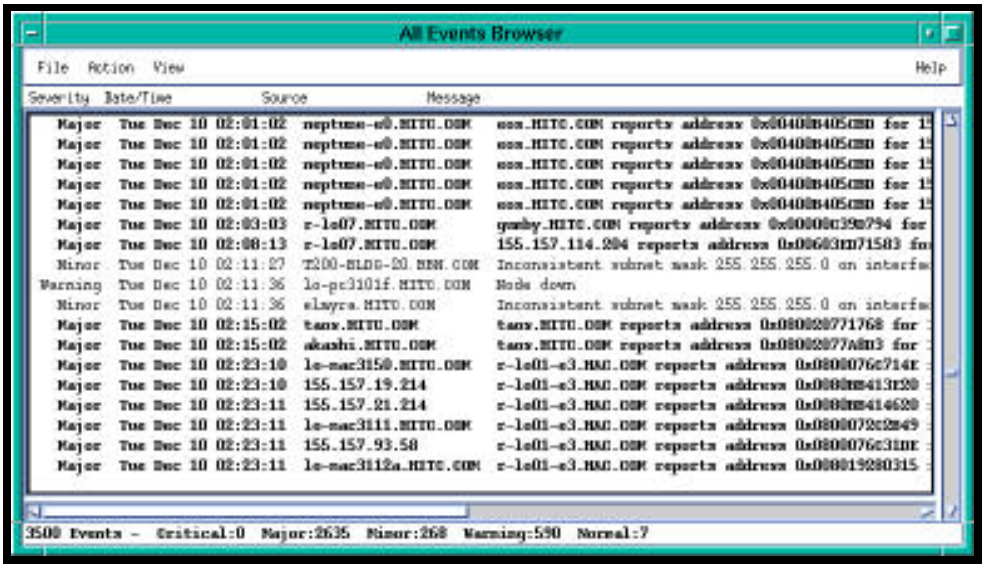

Figure 26. Events Browser Window

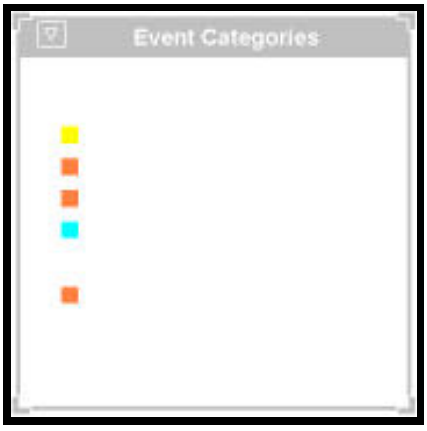

Figure 27. Event Categories Window

The default categories included in the Event Categories window are:

- **Error Events,** which indicate inconsistent or unexpected behavior.
- **Threshold Events**, which indicate that a threshold was exceeded.
- **Status Events**, which indicates that an object or interface status changed to "up" or "down," or an object or interface started or stopped responding to Internet control message protocol (ICMP) echo requests.
- **Configuration Events**, which indicate a node's configuration changed.
- **Application Alert Events,** which indicate an HP OpenView Windows application generated an alarm or alert.
- **All Events**, which indicates one or more of the previously listed events occurred. Selecting this button lists all events in the listed categories and others in one dialog box.

To check for event notifications, examine the Event Categories window to observe any color change in one or more of the buttons for the event categories. If there is a color change, you can click on the button to view its associated Events Browser window. For example, suppose you are monitoring the network when a critical threshold is exceeded somewhere on the network.

*In the following example the **Threshold Events** button is red, which indicates that a critical threshold was exceeded somewhere on the network.*

Checking for Events Notifications Procedure

1 Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list.

- Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message.

2 To view the node that generated the event shown in this example, select the event from the list and click on **Action→Highlight Source on Map.**

- A map will appear with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.

3 To delete the event, select the event and click on **Action → Delete → Selected Event.**

- This will delete only the selected event.

For more information about event notification, click on the **help** button in the dialog box for the event being viewed or select **View SNMP Events** from the **Help: Index → Task.**

Practical Exercises

Practical Exercises

Introduction

These exercises are designed to practice key elements of the Network Administration procedures. Perform the tasks identified in each set of exercises.

Equipment and Materials

A functioning ECS system.

These exercises are all subject to updating following my participation in an HPOV training class.

Starting an NNM Session

1. Start an NNM session.

Viewing Current Network and System Configuration, Network Address Information, and How Traffic is Routed on the Network

1. Determine the layout of the current network.
2. What is the Network address of the following interfaces:

   interface #1

   interface #2

   interface #3

3. What is the Gateway through which the following Destinations are routed:

   interface #1

   interface #2

   interface #3

Adding Network, Segment, and IP Interface Objects

1. Add ***insert-network-object-here*** to the network layout.
2. Add ***insert-segment-object-here*** to the network layout.
3. Add ***insert-IP-interface-object-here*** to the network layout.

NOTE: Specifics on these practical exercises are all TBA depending on the network layout. I won't be able to complete this portion until I have an opportunity to get some hands-on time with the network.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

This page intentionally left blank.